(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
12 avril 2001 (12.04.2001)

PCT

(10) Numéro de publication internationale
WO 01/26279 A1

(51) Classification internationale des brevets[7]: H04L 9/32

(21) Numéro de la demande internationale:
PCT/FR00/02717

(22) Date de dépôt international:
29 septembre 2000 (29.09.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:

99/12465	1 octobre 1999 (01.10.1999)	FR
99/12467	1 octobre 1999 (01.10.1999)	FR
99/12468	1 octobre 1999 (01.10.1999)	FR
00/09644	21 juillet 2000 (21.07.2000)	FR

(71) Déposants *(pour tous les États désignés sauf US)*: **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). **TELEDIFFUSION DE FRANCE** [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75732 Paris Cedex 15 (FR). **MATH RIZK** [BE/BE]; Verte Voie, Boîte 5, B-1348 Louvain-la-Neuve (BE).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)*: **GUILLOU, Louis** [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarre (FR). **QUISQUATER, Jean-Jacques** [BE/BE]; 3, avenue des Canards, B-1640 Rhode Saint Genese (BE).

(74) Mandataire: **VIDON, Patrice**; Le Nobel, 2, allée Antoine Becquerel, BP 90 333, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)*: brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée:
— *Avec rapport de recherche internationale.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: METHOD, SYSTEM, DEVICE FOR PROVING AUTHENTICITY OF AN ENTITY OR INTEGRITY OF A MESSAGE

(54) Titre: PROCEDE, SYSTEME, DISPOSITIF A PROUVER L'AUTHENTICITE D'UNE ENTITE OU L'INTEGRITE D'UN MESSAGE

(57) Abstract: The invention concerns a method whereby the proof is established by: m (≥ 1) pairs of private Q_i and public $G_i = g_i^2$ values; a public module n formed by the product of f(≥ 2) prime factors; an exponent $v = 2^k$ ($k > 1$), linked by the relationships of the type: $G_i . Q_i^v \equiv 1$. mod n or $G_i \equiv Q_i^v$ mod n. Among the m numbers obtained by increasing Q_i or its inverse modulo n to modulo n square, k-1 times rank, at least one of them is different from $\pm g_i$. Among the 2m equations: $x^2 \equiv g_i$ mod n, $x^2 \equiv -g_i$ mod n, at least one of them has solutions in x in the ring of modulo n integers.

(57) Abrégé: La preuve est établie au moyen de: m (≥ 1) couples de valeurs privées Q_i et publiques $G_i = g_i^2$, un module public n constitué par le produit de f (≥ 2) facteurs premiers, un exposant $v = 2^k$ ($k > 1$), liés par des relations du type: $G_i.Q_i^v \equiv 1$.mod n ou $G_i \equiv Q_i^v$ mod n. Parmi les m nombres obtenus en élevant Q_i ou son inverse modulo n au carré modulo n, k-1 fois de rang, au moins l'un d'entre eux est différent de $\pm g_i$. Parmi les 2m équations: $x^2 \equiv g_i$ mod n; $x^2 \equiv -g_i$ mod n, au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n.

WO 01/26279 A1